



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/062,853	01/31/2002	James Kleinsteinber	112-0019US	1224

29855 7590 08/17/2007
WONG, CABELLO, LUTSCH, RUTHERFORD & BRUCCULERI,
L.L.P.
20333 SH 249
SUITE 600
HOUSTON, TX 77070

EXAMINER

BROWN, CHRISTOPHER J

ART UNIT	PAPER NUMBER
----------	--------------

2134

MAIL DATE	DELIVERY MODE
-----------	---------------

08/17/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/062,853	Applicant(s) KLEINSTEIBER ET AL.	
	Examiner Christopher J. Brown	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 June 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-50 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-50 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

Applicant's arguments, filed 6/13/2007 with respect to the rejection(s) of claim(s) 1-50 under USC 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Shelest US 7,134,019

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 1-19, 21-32, 34-53 is rejected under 35 U.S.C. 103(a) as being unpatentable over Li US 5,473,599 in view of "Entity Authentication using public key cryptography" William Daley in view of Shelest US 7,134,019

As per claim 1, Li teaches a system of routers that communicate through hello messages and include authentication messages, (Col 3 lines 1-4, Col 10 line 65-Col 11 line 16). Li does not teach a strong authentication system.

Daley teaches a strong authentication protocol comprising: sending a secret fact (random nonce) from sender B to a receiver A, (page 21, 23). Daley states receiving a second type derivative (signature of A) of said first secret fact, pre-defined information (certificate of A with key information). Daley teaches that

receiver B verifies second type derivative and secret fact, (page 23). Daley teaches that receiver B verifies the certificate or chain of certificates (page 23).

It would have been obvious to one of ordinary skill in the art to use the authentication system of Daley with the routers of Li, because the strong authentication would enhance the security of the routers.

Shelest teaches sending predefined information (authenticated message 500, similar to a certificate) that includes predefined information (PKD address, Public Key, Time Stamp) (Col 7 lines 23-28). Shelest teaches sending a third type derivative of said pre-defined information about said second switch being generated by the second switch (hash/signature of PKD address and timestamp) (Col 7 lines 40-47). Shelest teaches the recipient verifies the pre-defined information by comparison (Col 8 lines 5-12).

It would have been obvious to one of ordinary skill in the art to use the message/certificate of Shelest because it allows authentication without need for a third party, and the timestamp prevents replay attacks.

As per claim 2, Li teaches the routers use the same protocols, which use the same ports, (Col 8 lines 4-7).

As per claims 3, and 4, Daley teaches verifying the digital signature, which includes reversing (decryption) and creating (hashing).

As per claim 5, Daley teaches that second type derivative is associated with second switch (A) (page 23).

As per claim 6, Shelest teaches the third type derivative is specific to both the first and second switches (hash/signature of PKD address, and id of recipient) (Col 7 lines 40-50).

As per claim 7, , Daley and Shelest teach defined information is a certificate that includes encryption key information, (Daley pg 23), (Shelest Col 7 lines 40-50).

As per claims 8, 9, 24, 25, 38, 39, and 52 Daley teaches sending a one time random number as a first secret fact, (pg 22).

As per claims 10, 23, 37, 50, and 51 Li teaches a system of routers that communicate through hello messages and include authentication messages, (Col 3 lines 1-4, Col 10 line 65-Col 11 line 16). Li does not teach a strong authentication system.

Daley teaches a strong authentication protocol comprising: sending a secret fact (random nonce B) from sender B to a receiver A, (page 21, 23). Daley states receiving a second type derivative (signature of A) of said first fact, pre-defined information (certificate/message of A with key information), and second fact (random nonce A). Daley teaches that B creates a first-type derivative (signature of B) of said second fact, and sends it to A, (page 24). Daley teaches B sending first-type derivative, defined information (certificate/message of B with key information, and third type derivative), to A(pg 21, 24. Daley teaches A verifies first type derivative, and B verifies second type derivative. Daley teaches both A and B verify the third type derivative.

Art Unit: 2134

It would have been obvious to one of ordinary skill in the art to use the authentication system of Daley with the routers of Li, because the strong authentication would enhance the security of the routers.

Shelest teaches sending defined information (authenticated message 500, similar to a certificate) that includes defined information (PKD address, Public Key, Time Stamp) (Col 7 lines 23-28). Shelest teaches sending a third type derivative of said pre-defined information about said second switch being generated by the second switch (hash of PKD address and timestamp) (Col 7 lines 40-47). Shelest teaches the recipient verifies the pre-defined information by comparison (Col 8 lines 5-12).

It would have been obvious to one of ordinary skill in the art to use the message/certificate of Shelest because it allows authentication without need for a third party, and the timestamp prevents replay attacks.

As per claim 11, Daley teaches verifying the digital signature, which includes reversing (decryption) and comparing.

As per claim 12, Daley teaches verifying the signature which includes creating (hashing) and comparing.

As per claims 13, 14, 15, 26, 27, 28, 40, 41, and 42, Daley teaches creating a second type derivative by creating a signature of a first fact. Schneier provides the method of creating a signature which is well known in the art. The method of

Art Unit: 2134

which includes hashing the first fact and encrypting said hash with a private key, (Schneier pg 38-39).

As per claims 16, 29, and 43, Daley and Shelest teach defined information is a certificate that includes encryption key information, (Daley pg 23), (Shelest Col 7 lines 40-50).

As per claims 17, 30, and 44, , Daley and Shelest teach defined information is a certificate that includes public encryption key information, (Daley pg 23), (Shelest Col 7 lines 40-50).

As per claims 18, 31, and 45 Shelest teaches the third type derivative is specific to both the first and second switches (hash/signature of PKD address, and id of recipient) (Col 7 lines 40-50).

As per claims 19, 32, and 46 Shelest teaches sending a third type derivative of said pre-defined information about said second switch being generated by the second switch (signature and hash of PKD address and timestamp) (Col 7 lines 40-50).

As per claims 21, 22, 34, 35, 36, 47, 48, and 49). Shelest teaches the recipient reverses the third type derivative (reverses signature created from private key) and verifies the pre-defined information by comparison (Col 8 lines 5-12).

Art Unit: 2134

Claims 20, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Li US 5,473,599 in view of “Entity Authentication using public key cryptography” William Daley in view of Shelest US 7,134,019 in view of JP02001148697A

As per claims 20 and 33, Li teaches a system of routers that communicate through hello messages and include authentication messages, (Col 3 lines 1-4, Col 10 line 65-Col 11 line 16). Li does not teach a strong authentication system.

Daley teaches that receiver B verifies the certificate (page 23).

would have been obvious to one of ordinary skill in the art to use the authentication system of Daley with the routers of Li, because the strong authentication would enhance the security of the routers.

Shelest teaches sending a third type derivative of said pre-defined information about said second switch being generated by the second switch (signature and hash of PKD address and timestamp using private key) (Col 7 lines 40-50).

Neither Li, Daley or Shelest teach that the authority is the manufacturer of the device.

JP02001148687 teaches a manufacturer stores a certificate and manufacturer signature made by a private key on each device. (Abstract).

It would have been obvious to one of ordinary skill in the art to use the method of JP02001148697 because it allows every device to communicate safely over a channel with low reliability.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher J. Brown



8/15/07


KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER